# An Intuitionistic Linear Logical Semantics of SAND Attack Trees

Harley Eades III

Computer Science
Augusta University
harley.eades@gmail.com

**Abstract.** TODO

## 1 Introduction

## 2 A Quaternary Semantics for SAND Attack Trees

Kordy et al. [1] gave a very elegant and simple semantics of attack-defense trees in boolean algebras. Unfortunately, while their semantics is elegant it does not capture the resource aspect of attack trees, it allows contraction, and it does not provide a means to model sequential conjunction. In this section we give a semantics of attack trees in the spirit of Kordy et al.'s using a four valued logic.

The propositional variables of our ternary logic, denoted by $A$, $B$, $C$, and $D$, range over the set $\mathsf{Four} = \{0, \frac{1}{4}, \frac{1}{2}, 1\}$. We think of 0 and 1 as we usually do in boolean algebras, but we think of $\frac{1}{4}$ and $\frac{1}{2}$ as intermediate values that can be used to break various structural rules. In particular we will use these values to prevent exchange for sequential conjunction from holding, and contraction from holding for parallel and sequential conjunction.

**Definition 1.** *The logical connectives of our four valued logic are defined as follows:*

*Parallel Conjunction:*

$$\begin{array}{l} A \odot_4 B = 1, \textit{where neither } A \textit{ nor } B \textit{ are } 0 \\ A \odot_4 B = 0, \textit{otherwise} \end{array}$$

*Sequential Conjunction:*

$$\begin{array}{l} \frac{1}{4} \rhd_4 B = \frac{1}{4}, \textit{where } B \neq 0 \\ A \rhd_4 B = 1, \textit{where } A \in \{\frac{1}{2}, 1\} \textit{ and } B \neq 0 \\ A \rhd_4 B = 0, \textit{otherwise} \end{array}$$

*Choice:* $A \sqcup_4 B = \mathsf{max}(A, B)$

These definitions are carefully crafted to satisfy the necessary properties to model attack trees. Comparing these definitions with Kordy et al.'s [1] work we can see that choice is defined similarly, but parallel conjunction is not a product – ordinary conjunction – but

rather a linear tensor product, and sequential conjunction is not actually definable in a boolean algebra, and hence, makes heavy use of the intermediate values to insure that neither exchange nor contraction hold. The following results solidify these claims.

We use the usual notion of equivalence between propositions, that is, propositions $\phi$ and $\psi$ are considered equivalent, denoted by $\phi \equiv \psi$, if and only if they have the same truth tables. In order to model attack trees the previously defined logical connectives must satisfy the appropriate equivalences corresponding to the equations between attack trees. These equivalences are all proven by the following results.

**Lemma 1 (Parallel Conjunction).**

*(Symmetry) For any A and B,* $A \odot_4 B \equiv B \odot A$.

*(Associativity) For any A, B, and C,* $(A \odot_4 B) \odot_4 C \equiv A \odot_4 (B \odot_4 C)$.

*(Contraction) It is not the case that for any A,* $A \odot_4 A \equiv A$.

*Proof.* Symmetry and associativity hold by simply comparing truth tables. As for contraction, suppose $A = \frac{1}{4}$. Then by definition $A \odot_4 A = 1$, but $\frac{1}{4}$ is not 1.

**Lemma 2 (Sequential Conjunction).**

*(Symmetry) It is not the case that for any A and B,* $A \rhd_4 B \equiv B \rhd_4 A$.

*(Associativity) For any A, B, and C,* $(A \rhd_4 B) \rhd_4 C \equiv A \rhd_4 (B \rhd_4 C)$.

*(Conjunction) It is not the case that for any A,* $A \rhd_4 A \equiv A$.

*Proof.* First, we prove symmetry fails. Suppose $A = \frac{1}{4}$ and $B = \frac{1}{2}$. Then $A \rhd_4 B = \frac{1}{4}$, but $B \rhd_4 A = \frac{1}{2}$. Associativity holds by simply comparing truth tables. As for contraction, suppose $A = 1$. Then by definition $A \odot A = \frac{1}{2}$, but $\frac{1}{2}$ is not 1.

**Lemma 3 (Choice).**

*(Symmetry) For any A and B,* $A \sqcup_4 B \equiv B \sqcup_4 A$.

*(Associativity) For any A, B, and C,* $(A \sqcup_4 B) \sqcup_4 C \equiv A \sqcup_4 (B \sqcup_4 C)$.

*(Contraction) For any A,* $A \sqcup_4 A \equiv_4 A$.

*Proof.* Each case of this proof holds by simply comparing truth tables.

**Lemma 4 (The Distributive Laws).**

*i. For any A, B, and C,* $A \odot_4 (B \sqcup_4 C) \equiv (A \odot_4 B) \sqcup_4 (A \odot_4 C)$.

*ii. For any A, B, and C,* $(A \sqcup_4 B) \odot_4 C \equiv (A \odot_4 C) \sqcup_4 (B \odot_4 C)$.

*iii. For any A, B, and C,* $A \rhd_4 (B \sqcup_4 C) \equiv (A \rhd_4 B) \sqcup_4 (A \rhd_4 C)$.

*iv. For any A, B, and C,* $(A \sqcup_4 B) \rhd_4 C \equiv (A \rhd_4 C) \sqcup_4 (B \rhd_4 C)$.

*Proof.* This proof holds by simply comparing truth tables.

At this point it is quite easy to model attack trees as formulas. The following defines their interpretation.

**Definition 2.** *Suppose* $\mathbb{B}$ *is some set of base attacks, and* $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ *is an assignment of base attacks to propositional variables. Then we define the interpretation of* ATerms *to propositions as follows:*

$$\begin{array}{ll} [\![\mathbf{b} \in \mathbb{B}]\!] & = \alpha(\mathbf{b}) \\ [\![\mathsf{AND}\, T_1\, T_2]\!] & = [\![T_1]\!] \odot_4 [\![T_2]\!] \\ [\![\mathsf{SAND}\, T_1\, T_2]\!] & = [\![T_1]\!] \rhd_4 [\![T_2]\!] \\ [\![\mathsf{OR}\, T_1\, T_2]\!] & = [\![T_1]\!] \sqcup_4 [\![T_2]\!] \end{array}$$

We can use this semantics to prove equivalences between attack trees.

**Lemma 5 (Equivalence of Attack Trees in the Ternary Semantics).** *Suppose* $\mathbb{B}$ *is some set of base attacks, and* $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ *is an assignment of base attacks to propositional variables. Then for any attack trees* $T_1$ *and* $T_2$, $T_1 \approx T_2$ *if and only if* $[\![T_1]\!] \equiv [\![T_2]\!]$.

*Proof.* This proof holds by induction on the form of $T_1 \approx T_2$.

This is a very simple and elegant semantics, but it also leads to a more substantial theory.

## 3 Lineale Semantics for SAND Attack Trees

Classical natural deduction has a semantics in boolean algebras, and so the semantics in the previous section begs the question of whether there is a natural deduction system that can be used to reason about attack trees. We answer this question in the positive, but before defining the logic we first build up a non-trivial concrete categorical model of our desired logic in dialectica spaces, but this first requires the abstraction of the quaternary semantics into a preorder semantics we call the lineale semantics of SAND attack trees. This semantics will live at the base of the dialectica space model given in the next section, but it also begins to shed light on new and interesting reasoning tools for attack trees.

We denote by $\leq_4$: $\mathsf{Four} \times \mathsf{Four} \to \mathsf{Four}$ the obvious preorder on Four making $(\mathsf{Four}, \leq_4)$ a preordered set (proset). It is well known that every preordered set induces a category whose objects are the elements of the carrier set, here Four, and morphisms $\mathsf{Hom}_{\mathsf{Four}}(a, b) = a \leq_4 b$. Composition of morphisms hold by transitivity and identities exists by reflexivity. Under this setting it is straightforward to show that for any propositions $\phi$ and $\psi$ over Four we have $\phi \equiv \psi$ if and only if $\phi \leq_4 \psi$ and $\psi \leq_4 \phi$. Thus, every result proven for the logical connectives on Four in the previous section induce properties on morphisms in this setting.

In addition to the induced properties just mentioned we also have the following new ones which are required when lifting this semantics to dialectica spaces, but are also important when building a corresponding logic.

**Lemma 6 (Functorality).**

*(Parallel Conjunction) For any A, B, C, and D, if* $A \leq_4 C$ *and* $B \leq_4 D$*, then* $(A \odot_4 B) \leq_4 (C \odot_4 D)$.

*(Sequential Conjunction) For any A, B, C, and D, if* $A \leq_4 C$ *and* $B \leq_4 D$*, then* $(A \rhd_4 B) \leq_4 (C \rhd_4 D)$.

*(Choice) For any A, B, C, and D, if* $A \leq_4 C$ *and* $B \leq_4 D$*, then* $(A \sqcup_4 B) \leq_4 (C \sqcup_4 D)$.

*Proof.* Part one holds by a straightforward case analysis on $A$, $B$, $C$, and $D$. In any cases where $(A \odot_4 B) \leq_4 (C \odot_4 D)$ does not hold, then one of the premises will also not hold. The other cases are similar.

The logic we a building up is indeed intuitionistic, but none of the operators we have introduced thus far are closed, but we can define the standard symmetric linear tensor product in Four that is closed.

**Definition 3.** *The following defines the linear tensor product on* Four *as well as linear implication:*

$$
\begin{array}{ll}
A \otimes_4 B = \mathsf{max}(A, B), & A \multimap_4 B = 0, \textit{where } B <_4 A \\
\quad \textit{where } A \textit{ nor } B \textit{ are } 0 & A \multimap_4 A = A, \textit{where } A \in \{\frac{1}{4}, \frac{1}{2}\} \\
A \otimes_4 B = 0, \textit{otherwise} & A \multimap_4 B = 1, \textit{otherwise}
\end{array}
$$

*The unit of the tensor product is* $I_4 = \frac{1}{4}$.

The expected monoidal properties hold for the tensor product.

**Lemma 7 (Tensor is Symmetric Monoidal Closed).**

*(Symmetry) For any A and B,* $A \otimes_4 B \equiv B \otimes A$.

*(Associativity) For any A, B, and C,* $(A \otimes_4 B) \otimes_4 C \equiv A \otimes_4 (B \otimes_4 C)$.

*(Unitors) For any A,* $(A \otimes I_4) \equiv A \equiv (I_4 \otimes A)$.

*(Tensor is Functorial) For any A, B, C, and D, if* $A \leq_4 C$ *and* $B \leq_4 D$*, then* $(A \otimes_4 B) \leq_4 (C \otimes_4 D)$.

*(Implication is Functorial) For any A, B, C, and D, if* $C \leq_4 A$ *and* $B \leq_4 D$*, then* $(A \multimap_4 B) \leq_4 (C \multimap_4 D)$.

*(Closure) For any A, B, and C,* $(A \otimes_4 B) \leq_4 C$ *if and only if* $A \leq_4 (B \multimap_4 C)$.

*Proof.* The top three cases hold by simply comparing truth tables. Finally, the last three cases hold by a case analysis over $A$, $B$, $C$, and $D$. If at any time the conclusion is false, then one of the premises will also be false.

We now define lineales which depend on the notion of a monoidal proset. The definition of lineales given here is a slight generalization over the original definition given by Hyland and de Paiva – see Definition 1 of [**?**]. They base lineales on posets instead of prosets, but the formalization given here shows that anti-symmetry can be safely dropped.

**Definition 4.** *A **monoidal proset** is a proset, $(L, \leq)$, with a given symmetric monoidal structure $(L, \circ, e)$. That is, a set $L$ with a given binary relation $\leq\colon L \times L \to L$ satisfying the following:*

- *(reflexivity) $a \leq a$ for any $a \in L$*
- *(transitivity) If $a \leq b$ and $b \leq c$, then $a \leq c$*

*together with a monoidal structure $(\circ, e)$ consisting of a binary operation, called multiplication, $\circ : L \times L \to L$ and a distinguished element $e \in L$ called the unit such that the following hold:*

- *(associativity) $(a \circ b) \circ c = a \circ (b \circ c)$*
- *(identity) $a \circ e = a = e \circ a$*
- *(symmetry) $a \circ b = b \circ a$*

*Finally, the structures must be compatible, that is, if $a \leq b$, then $a \circ c \leq b \circ c$ for any $c \in L$.*

Now a lineale can be seen as essentially a symmetric monoidal closed category in the category prosets.

**Definition 5.** *A **lineale** is a monoidal proset, $(L, \leq, \circ, e)$, with a given binary operation, called implication, $\multimap\colon L \times L \to L$ such that the following hold:*

- *(relative complement) $(a \multimap b) \circ a \leq b$*
- *(adjunction) If $a \circ y \leq b$, then $y \leq a \multimap b$*

The set $\mathsf{2} = \{0, 1\}$ is an example of a lineale where the order is the usual one, the multiplication is boolean conjunction, and the implication is boolean implication. This example is not that interesting, because $\mathsf{2}$ is a boolean algebra. An example of a proper lineale can be given using the three element set $\mathsf{Three} = \{0, \frac{1}{2}, 1\}$, but one must be careful when defining lineales, because it is possible to instead define Heyting algebras, and hence, become nonlinear.

Given the operations and properties shown for $(\mathsf{Four}, \leq_4)$ above we can easily prove that $(\mathsf{Four}, \leq_4)$ defines a lineale.

**Lemma 8.** *The proset, $(\mathsf{Four}, \leq_4, \otimes_4, I_4, \multimap_4)$ is a lineale.*

*Proof.* First, $(\mathsf{Four}, \leq_4, \otimes_4, I_4)$ defines a monoidal proset, because the tensor product is associative, $I_4$ is the identity, and symmetric by Lemma 7. We can also show that the tensor product is compatible, that is, if $A \leq_4 B$, then $(A \otimes_4 C) \leq_4 (B \otimes C)$ for any $C$. Suppose $A \leq_4 B$, then by reflexivity we also know that $C \leq_4 C$. Thus, by functorality, Lemma 7, we obtain our result.

Finally, we show that $(\mathsf{Four}, \leq_4, \otimes_4, I_4, \multimap_4)$ is a lineale. The adjunction property already holds by Lemma 7, thus, all that is left to show is that the relative complement holds. We know by Lemma 7 that for any $A$, $B$, and $C$, if $A \leq_4 (B \multimap_4 C)$, then $(A \otimes_4 B) \leq_4 C$. In addition, we know by reflexivity that $(A \multimap_4 B) \leq_4 (A \multimap_4 B)$, thus by the previous property we obtain that $((A \multimap_4 B) \otimes_4 A) \leq_4 B$.

The interpretation of attack trees into the lineale $(\mathsf{Four}, \leq_4, \otimes_4, I_4, \multimap_4)$ does not change from Definition 2, but the equivalences between attack trees, Lemma 5, can be abstracted.

**Lemma 9 (Equivalence of Attack Trees in the Lineale Semantics).** *Suppose $\mathbb{B}$ is some set of base attacks, and $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ is an assignment of base attacks to propositional variables. Then for any attack trees $T_1$ and $T_2$, $T_1 \approx T_2$ if and only if $[\![T_1]\!] \leq_4 [\![T_2]\!]$ and $[\![T_2]\!] \leq_4 [\![T_1]\!]$.*

*Proof.* This proof holds by induction on the form of $T_1 \approx T_2$.

This result seems basic, but has some interesting consequences. Notice that we can break up equivalence of attack trees, $T_1 \approx T_2$, into rewrite rules $T_1 \rightsquigarrow T_2$ and $T_1 \leftsquigarrow T_2$ by reading each equivalence from left-to-right and right-to-left respectively, such that, $T_1 \approx T_2$ if and only if $T_1 \rightsquigarrow^* T_2$ and $T_1 \leftsquigarrow^* T_2$. Then we have the following corollary.

**Corollary 1 (Simplifications of Attack Trees in the Lineale Semantics).** *Suppose $\mathbb{B}$ is some set of base attacks, and $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ is an assignment of base attacks to propositional variables. Then for any attack trees $T_1$ and $T_2$ the following hold:*

*i. if $T_1 \rightsquigarrow T_2$, then $[\![T_1]\!] \leq_4 [\![T_2]\!]$*
*ii. if $T_1 \leftsquigarrow T_2$, then $[\![T_2]\!] \leq_4 [\![T_1]\!]$*

More generally, the previous two results show that equivalence of attack trees can actually be modeled by isomorphisms in the category, and that if we break the equivalences up into rewrite rules, then rewriting attack trees corresponds to exhibiting a morphism in the category.

The previous corollary also has practical consequences. The left-to-right rewrite rules, what we call the attack tree simplification rules, can be used to normalize attack trees, we discuss this in more detail in Section **??**, such that, if two attack trees have the same normal form, then they are equivalent. The previous corollary implies that doing so is semantically valid.

Finally, the previous two results lead us to a more logical viewpoint. If we know $[\![T_1]\!] \leq_4 [\![T_2]\!]$, then by closure $I_4 \leq_4 ([\![T_1]\!] \multimap_4 [\![T_2]\!])$. Thus, two attack trees are then equivalent if and only if they are bi-conditionally related, i.e. $I_4 \leq_4 ([\![T_1]\!] \multimap_4 [\![T_2]\!])$ and $I_4 \leq_4 ([\![T_2]\!] \multimap_4 [\![T_1]\!])$. Therefore, if we are able to find a logic that is sound with respect to the semantics laid out thus far, then we can use it to reason about attack trees using linear implication, but can we first define a non-trivial – not in prosets – categorical model of attack trees?

## 4 Dialectica Semantics of SAND Attack Trees

In her thesis de Paiva [**?**] gave one of the first sound and complete categorical models, called dialectica categories, of full intuitionistic linear logic. Her models arose from giving a categorical definition to Gödel's Dialectica interpretation. de Paiva defines a particular class of dialectica categories called *GC* over a base category *C*, see page 41 of [**?**]. She later showed that by instantiating *C* to $\mathsf{Sets}$, the category of sets and total functions, that one arrives at concrete instantiation of *GC* she called $\mathsf{Dial}_2(\mathsf{Sets})$ whose objects are called *dialectica spaces*, and then she abstracts $\mathsf{Dial}_2(\mathsf{Sets})$ into a family of concrete dialectica spaces, $\mathsf{Dial}_L(\mathsf{Sets})$, by replacing $\mathsf{2}$ with an arbitrary lineale *L*.

In this section we construct the dialectica category, $\mathsf{Dial}_4(\mathsf{Sets})$, and show that it is a model of attack trees. This will be done by essentially lifting each of the attack tree operators defined for the lineale semantics given in the previous section into the dialectica category. Working with dialectica categories can be very complex due to the nature of how they are constructed. In fact, they are one of the few examples of theories that are easier to work with in a proof assistant than outside of one. Thus, throughout this section we only give brief proof sketches, but the interested reader will find the complete proofs in the formalization.

## References

1. Barbara Kordy, Marc Pouly, and Patrick Schweitzer. Computational aspects of attack–defense trees. In Pascal Bouvry, MieczysławA. Kłopotek, Franck Leprévost, Małgorzata Marciniak, Agnieszka Mykowiecka, and Henryk Rybiński, editors, *Security and Intelligent Information Systems*, volume 7053 of *Lecture Notes in Computer Science*, pages 103–116. Springer Berlin Heidelberg, 2012.

## Appendix